Algebraic Quantum Synchronizable Codes

K. Guenda, G. G. La Guardia and T. A. Gulliver*

Abstract

In this paper, we construct quantum synchronizable codes (QSCs) based on the sum and intersection of cyclic codes. Further, infinite families of QSCs are obtained from BCH and duadic codes. Moreover, we show that the work of Fujiwara [7] can be generalized to repeated root cyclic codes (RRCCs) such that QSCs are always obtained, which is not the case with simple root cyclic codes. The usefulness of this extension is illustrated via examples of infinite families of QSCs from repeated root duadic codes. Finally, QSCs are constructed from the product of cyclic codes.

1 Introduction

The main goal of frame synchronization in communication systems is to ensure that information block boundaries can be correctly determined at the receiver. To achieve this goal, numerous synchronization techniques have been developed for classical communication systems. However, these techniques are not applicable to quantum communication systems since a qubit measurement typically destroys the quantum states and thus also the corresponding quantum information. To circumvent this problem, synchronization can be achieved using a classical system external to the quantum system, but such a solution does not take advantage of the benefits that quantum processing can provide.

In a landmark paper [7], Fujiwara provided a framework for quantum block synchronization. The approach is to employ codes, called quantum synchronizable codes (QSCs), which allow the identification of codeword boundaries without destroying the quantum states. This is achieved by determining how many qubits from proper alignment the system is should misalignment occur. More precisely, an $(a_l, a_r) - [[n,k]]_2$ QSC is an $[[n,k]]_2$ code that encodes k logical qubits into a physical qubit, and corrects misalignments of up to a_l qubits

*K. Guenda is with the Faculty of Mathematics USTHB, University of Science and Technology of Algiers, Algeria. G. G. La Guardia is with Department of Mathematics and Statistics, State University of Ponta Grossa (UEPG), 84030-900, Ponta Grossa, PR, Brazil. T. A. Gulliver is with the Department of Electrical and Computer Engineering, University of Victoria, PO Box 1700, STN CSC, Victoria, BC, Canada V8W 2Y2 email: kguenda@usthb.dz, agullive@ece.uvic.ca.

to the left and up to a_r qubits to the right. These quantum codes may correct more phase errors than bit errors. This is an advantage because, as shown by Ioffe and Mézard [14], in physical systems the noise is typically asymmetric so that bit errors occur less frequently than phase errors. Thus, one can consider QSCs as asymmetric quantum codes.

The initial work by Fujiwara was improved in [8] by making more extensive use of finite algebra to obtain block QSCs. Several QSC constructions have recently been presented [9, 23, 24]. These constructions employ BCH codes, cyclic codes related to finite geometries, punctured Reed-Muller codes, and quadratic residue codes and duadic codes of length p^n. Fujiwara and Vandendriessche [9] noted that "One of the main hurdles in the theoretical study of quantum synchronizable codes is that it is quite difficult to find suitable classical error-correcting codes because the required algebraic constraints are very severe and difficult to analyze." In this paper, quantum synchronizable codes are constructed based on the sum and intersection of cyclic codes. Further, we construct infinite families of quantum synchronizable codes from BCH and duadic codes. Moreover, the work of Fujiwara [7] is generalized to repeated root cyclic codes (RRCCs) such that a QSC is always obtained, which is not the case with simple root cyclic codes. The usefulness of this extension is illustrated with examples of infinite families of QSCs from repeated root duadic codes. Finally, we construct QSCs from the product of cyclic codes.

The remainder of this paper is organized as follows. In Section 2, some preliminary results and definitions are provided. Section 3 presents several new constructions of QSCs. More specifically, new families of QSCs are derived from the sum and intersection of cyclic codes, and from BCH codes, duadic codes, and repeated root cyclic codes (RRCCs). The construction of good QSCs given by Fujiwara is extended to RRCCs. In Section 4, QSCs are constructed from the product of cyclic codes.

2 Preliminary Results

Before presenting the constructions of QSCs, we recall some preliminary results which will be used in the next section.

Lemma 2.1 *[18, Lemma 3.1] Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of degree $m \geq 1$ with $f(0) \neq 0$. Then there exists a positive integer $e \leq q^m - 1$ such that $f(x)|(x^e - 1)$.*

From Lemma 2.1 the order of a nonzero polynomial is defined as follows.

Definition 2.2 *[18, Definition 3.2] Let $f(x) \in \mathbb{F}_q[x]$ be a nonzero polynomial. If $f(0) \neq 0$, the* order *of $f(x)$, denoted by* $\mathrm{ord}(f)$*, is defined as the smallest positive integer such that $f(x)|(x^e - 1)$. If $f(0) = 0$, then $f(x) = x^h g(x)$ where $h \in \mathbb{N}$ and $g(x) \in \mathbb{F}_q[x]$ with $g(0) \neq 0$ are uniquely determined. In this case,* $\mathrm{ord}(f)$*, is defined to be* $\mathrm{ord}(g)$.

The following results are well known.

Lemma 2.3 *[19, Theorem 4] Let C be a cyclic code of length n over $\mathbb{F}_q$ generated by $g(x)$. Then the dual code $C^\perp$ of C is generated by $g^\perp(x) = \frac{x^n-1}{g^*(x)}$ where $g^*(x) = x^{\deg(g(x))}g(x^{-1})$.*

Lemma 2.4 *If $f(x), g(x), h(x) \in \mathbb{F}_q[x]$ such that $f(x) = g(x)h(x)$, then $f^*(x) = g(x)^*h^*(x)$.*

Proof. The result is obvious for constant polynomials. Assume that $\deg(g(x)) = m \geq 1$ and $\deg(h(x)) = n \geq 1$. Since $\deg(f(x)) = m + n$, it follows that $f^*(x) = x^{m+n}f(1/x) = x^m g(1/x)x^n h(1/x) = g(x)^*h^*(x)$. $\square$

Lemma 2.5 *[18, Lemma 3.6] Let $f(x) \in \mathbb{F}_q[x]$ with $f(0) \neq 0$ and m be a positive integer. Then $f(x)|(x^m - 1)$ if and only if $\mathrm{ord}(f)|m$. Further, if the minimal polynomial $M_1(x)$ divides $f(x)$ then $\mathrm{ord}(f) = m$.*

We recall the following result by Fujiwara [7].

Theorem 2.6 *[7, Theorem 1] Let C be a dual-containing $[n, k_1, d_1]$ cyclic code and D be a C-containing $[n, k_2, d_2]$ cyclic code with $k_1 < k_2$. Then, for any pair of nonnegative integers (a_l, a_r) satisfying $a_l + a_r < k_2 - k_1$, there exists an $(a_l, a_r) - [[n + a_l + a_r, 2k_1 - n]]$ QSC that corrects up to at least $\lfloor \frac{d_1-1}{2} \rfloor$ phase errors and up to at least $\lfloor \frac{d_2-1}{2} \rfloor$ bit errors.*

Theorem 2.6 was improved in terms of synchronization capability as follows.

Theorem 2.7 *[8, Lemma 3] Let C be a dual-containing $[n, k_1, d_1]$ cyclic code and let D be a C-containing $[n, k_2, d_2]$ cyclic code with $k_1 < k_2$. Assume that $h(x)$ and $g(x)$ are the generator polynomials of C and D, respectively. Define the polynomial $f(x)$ of degree $k_2 - k_1$ such that $h(x) = f(x)g(x)$ over $\mathbb{F}_2[x]/(x^n - 1)$. Then for any pair of nonnegative integers (a_l, a_r) satisfying $a_l + a_r < \mathrm{ord}(f(x))$, there exists an $(a_l, a_r) - [[n + a_l + a_r, 2k_1 - n]]$ QSC that corrects up to at least $\lfloor \frac{d_1-1}{2} \rfloor$ phase errors and up to at least $\lfloor \frac{d_2-1}{2} \rfloor$ bit errors.*

Remark 2.8

- *The quantum codes given in Theorem 2.6 may correct more phase errors than bit errors since the number of phase errors (resp. bit errors) is related to the minimum distance d_1 of the dual-containing code C (resp. to the minimum distance d_2 of the C-containing code D). As explained in Section 1, this is an advantage of QSCs.*

- *Ioffe and Mézard [14] showed that in physical systems the noise is typically asymmetric, i.e. bit errors occur less frequently than phase errors. Based on this fact, there has been significant interest in constructing good asymmetric quantum codes [6, 12, 15, 16, 21].*

- *The quantity $a_l + a_r$ in Theorem 2.7 is called the maximum tolerance magnitude of synchronization errors. From Lemma 2.5, this quantity is less than m and is maximal if the polynomial $h(x)$ in Theorem 2.7 is divisible by $M_1(x)$.*

3 New Quantum Synchronizable Codes

In this section, we present several new constructions of quantum synchronizable codes (QSCs). More precisely, we construct new families of QSCs from cyclic codes including duadic codes and BCH codes.

3.1 Quantum Synchronizable Codes from Cyclic Codes

We now present two constructions of QSCs from cyclic codes. The first one is based on the sum code of cyclic codes and the second is obtained by considering the intersection of cyclic codes.

Theorem 3.1 *Let $n \geq 3$ be an integer such that $\gcd(n, 2) = 1$ and suppose that $m = \operatorname{ord}_n(2)$. Let C_1 be an $[n, k_1, d_1]$ dual-containing cyclic code and let C_2 be an $[n, k_2, d_2]$ C_1-containing cyclic code. Further, let C_3 be an $[n, k_3, d_3]$ cyclic code and C_4 be an $[n, k_4, d_4]$ C_3-containing cyclic code such that $\deg(\gcd(g_2(x), g_4(x))) < \deg(\gcd(g_1(x), g_3(x)))$, where $g_i(x)$ is the generator polynomial of C_i, $i = 1, 2, 3, 4$. Then, for any pair of nonnegative integers (a_l, a_r) satisfying $a_l + a_r < \deg(\gcd(g_1(x), g_3(x))) - \deg(\gcd(g_2(x), g_4(x)))$, there exists an $(a_l, a_r) - [[n + a_l + a_r, n - 2\deg(\gcd(g_1(x), g_3(x)))]]$ QSC that corrects up to at least $\lfloor \frac{d-1}{2} \rfloor$ phase errors and up to at least $\lfloor \frac{d^*-1}{2} \rfloor$ bit errors, where d is the minimum distance of the code $C_1 + C_3$ and d^* is the minimum distance of the code $C_2 + C_4$.*

Proof. Since the codes C_1 and C_3 are cyclic, the sum code $C_1 + C_3 = \{c_1 + c_3 | c_1 \in C_1 \text{ and } c_3 \in C_3\}$ is also cyclic. Since $C_1 + C_3$ is generated by the polynomial $g(x) = \gcd(g_1(x), g_3(x))$, it follows that $C_1 \subset C_1 + C_3$, so $(C_1 + C_3)^{\perp} \subset C_1^{\perp}$. As C_1 is dual-containing, it follows that $(C_1 + C_3)^{\perp} \subset C_1^{\perp} \subset C_1 \subset C_1 + C_3$, i.e. the sum code $C_1 + C_3$ is also a dual-containing cyclic code.

Let $g_{\diamond}(x) = \gcd(g_2(x), g_4(x))$. As $g_2(x)|g_1(x)$ and $g_4(x)|g_3(x)$, it follows that $g_{\diamond}(x)|g(x)$, and hence the inclusion $C_1 + C_3 \subset C_2 + C_4$ holds, where $C_2 + C_4$ is also a cyclic code. From $\deg(g_{\diamond}(x)) < \deg(g(x))$, it follows that $C_1 + C_3 \subsetneq C_2 + C_4$. Applying Theorem 2.6 to the codes $C_1 + C_3$ and $C_2 + C_4$, a QSC is obtained with parameters $(a_l, a_r) - [[n + a_l + a_r, n - 2\deg(\gcd(g_1(x), g_3(x)))]]$, where $a_l + a_r < \deg(\gcd(g_1(x), g_3(x))) - \deg(\gcd(g_2(x), g_4(x)))$, and corrects up to at least $\lfloor \frac{d-1}{2} \rfloor$ phase errors and up to at least $\lfloor \frac{d^*-1}{2} \rfloor$ bit errors. □

Theorem 3.2 *Let $n \geq 3$ be an integer such that $\gcd(n, 2) = 1$ and suppose that $m = \operatorname{ord}_n(2)$. Let C_1 be an $[n, k_1, d_1]$ self-orthogonal cyclic code. Further, let C_2 and C_3 be two cyclic codes with parameters $[n, k_2, d_2]$ and $[n, k_3, d_3]$, respectively, such that $\{0\} \subsetneq C_3^{\perp} \subsetneq C_1 \cap C_2$. Then for any pair of nonnegative integers (a_l, a_r) satisfying $a_l + a_r < n - \deg(g_3(x)) - \deg(lcm(g_1(x), g_2(x)))$, there exists an $(a_l, a_r) - [[n + a_l + a_r, 2\deg(\operatorname{lcm}(g_1(x), g_2(x))) - n]]$*

QSC that corrects up to at least $\lfloor \frac{d-1}{2} \rfloor$ *phase errors and up to at least* $\lfloor \frac{d_3-1}{2} \rfloor$ *bit errors, where* d *is the minimum distance of the code* $(C_1 \cap C_2)^\perp$*, and* $g_i(x)$ *is the generator polynomial of* C_i*,* $i = 1, 2, 3$.

Proof. Since the codes C_1 and C_2 are cyclic, it follows that the code $C_1 \cap C_2$ is cyclic. Thus its dual code $(C_1 \cap C_2)^\perp$ is also cyclic. As $C_1 \cap C_2 \subset C_1$, the inclusion $C_1^\perp \subset (C_1 \cap C_2)^\perp$ holds. Since C_1 is self-orthogonal, then $C_1 \cap C_2 \subset C_1 \subset C_1^\perp \subset (C_1 \cap C_2)^\perp$, i.e. the code $C_1 \cap C_2$ is self-orthogonal. Hence $(C_1 \cap C_2)^\perp$ is a dual-containing cyclic code. As $C_3^\perp \subsetneq C_1 \cap C_2$, we know that $(C_1 \cap C_2)^\perp \subsetneq C_3$. The dimension of the corresponding quantum code is $2\deg(\mathrm{lcm}(g_1(x), g_2(x))) - n$ and $a_l + a_r < n - \deg(g_3(x)) - \deg(\mathrm{lcm}(g_1(x), g_2(x)))$. Applying Theorem 2.6 to the codes $(C_1 \cap C_2)^\perp$ and C_3, for any pair of nonnegative integers (a_l, a_r) satisfying $a_l + a_r < n - \deg(g_3(x)) - \deg(\mathrm{lcm}(g_1(x), g_2(x)))$, there exists an $(a_l, a_r) - [[n + a_l + a_r, 2\deg(\mathrm{lcm}(g_1(x), g_2(x))) - n]]$ QSC that corrects up to at least $\lfloor \frac{d-1}{2} \rfloor$ phase errors and up to at least $\lfloor \frac{d_3-1}{2} \rfloor$ bit errors. $\square$

3.2 Quantum Synchronizable Codes from BCH Codes

The class of BCH codes [3,4] has been extensively employed in the construction of quantum codes. In [8], primitive BCH codes were used to construct quantum synchonizable codes. In this section, quantum synchronizable codes are constructed from BCH codes that are not primitive. First, we recall some basic concepts regarding BCH codes.

Let $\gcd(n, q) = 1$. The q-cyclotomic coset (q-coset for short), of s modulo n is defined as $C_s = \{s, sq, \ldots, sq^{m_s-1}\}$, where $sq^{m_s} \equiv s \bmod n$. Let α be a primitive nth root of unity and $M_i(x)$ denote the minimal polynomial of α^i. With this notation, the class of BCH codes, which are a subclass of cyclic codes, can be defined as follows.

Definition 3.3 *A cyclic code of length* n *over* $\mathbb{F}_q$ *is a BCH code with design distance* δ *if for some* $b \geq 0$, $g(x) = \mathrm{lcm}\{M_b(x), M_{b+1}(x), \ldots, M_{b+\delta-2}(x)\}$*. The generator polynomial* $g(x)$ *of* C *can be expressed in terms of its defining set* $Z = C_b \cup C_{b+1} \cup \cdots \cup C_{b+\delta-2}$ *as* $g(x) = \prod_{z \in Z}(x - \alpha^z)$.

It is well-known from the BCH bound that the minimum distance of a BCH code is greater than or equal to its design distance δ.

Consider the following two useful results.

Proposition 3.4 *[1, Theorems 3 and 10] Let* n *be a positive integer such that* $\gcd(n, 2) = 1$ *and let* $m = \mathrm{ord}_n(2)$*. If* $2 \leq \delta \leq \delta_{max} = \lfloor \kappa \rfloor$*, where* $\kappa = \frac{n}{2^m-1}(2^{\lceil m/2 \rceil} - 1)$*, then the narrow-sense* $BCH(n, 2, \delta)$ *code contains its Euclidean dual* $BCH^\perp(n, 2, \delta)$*.*

Lemma 3.5 *[1, Lemmas 8 and 9] Let* $n \geq 1$ *be an integer such that* $\gcd(n, 2) = 1$ *and* $2^{\lfloor m/2 \rfloor} < n \leq 2^m - 1$*, where* $m = \mathrm{ord}_n(2)$*.*

(i) The 2-coset $\mathbb{C}_x$ has cardinality m for all x in the range $1 \le x \le n2^{\lceil m/2 \rceil}/(2^m - 1)$.

(ii) If x and y are distinct integers in the range $1 \le x, y \le \min\{\lfloor n2^{\lceil m/2 \rceil}/(2^m - 1) - 1 \rfloor, n - 1\}$ such that $x, y \not\equiv 0 \bmod 2$, then the 2-cosets of x and y mod n are disjoint.

We now construct the new QSCs.

Theorem 3.6 *Let $n \ge 3$ be an integer such that $\gcd(n, 2) = 1$ and suppose that $2^{\lfloor m/2 \rfloor} < n \le 2^m - 1$, where $m = \mathrm{ord}_n(2)$. Consider integers a and b such that $1 \le a < b < r = \min\{\lfloor n2^{\lceil m/2 \rceil}/(2^m - 1) - 1 \rfloor, n - 1, \lfloor \kappa \rfloor\}$, where $\kappa = \frac{n}{2^m - 1}(2^{\lceil m/2 \rceil} - 1)$ and $a, b \not\equiv 0 \bmod 2$. Then, for any pair of nonnegative integers (a_l, a_r) satisfying $a_l + a_r < m(t - u)$, there exists an $(a_l, a_r) - [[n + a_l + a_r, n - 2m(t + 1)]]$ QSC that corrects up to at least $\lfloor \frac{d-1}{2} \rfloor$ phase errors and up to at least $\lfloor \frac{d^*-1}{2} \rfloor$ bit errors, where $d \ge b + 1$, $d^* \ge a + 1$, $t = (b - 1)/2$ and $u = (a - 1)/2$.*

Proof. Let D be the binary narrow-sense BCH code of length n generated by the product of the minimal polynomials

$$D = \langle M_1(x) M_3(x) \cdots M_a(x) \rangle,$$

where $a = 2u + 1$ and $u \ge 0$ is an integer. Further, let C be the binary narrow-sense BCH code of length n generated by the product of the minimal polynomials

$$C = \langle M_1(x) M_3(x) \cdots M_b(x) \rangle,$$

where $b = 2t + 1$ and $t \ge 1$ is an integer. It then follows that $C \subset D$, and by Proposition 3.4 C is dual-containing. From Lemma 3.5 and a straightforward computation, the dimension of D is $k_2 = n - m(u + 1)$. Similarly, the dimension of C is $k_1 = n - m(t + 1)$. Thus, $k_2 - k_1 = m(t - u)$ and $2k_1 - n = n - 2m(t + 1)$. From the BCH bound, since the defining set of D contains a sequence of a consecutive integers, it follows that the minimum distance of D satisfies $d_2 \ge a + 1$. Analogously, since the defining set of C contains a sequence of b consecutive integers, from the BCH bound the minimum distance of C satisfies $d_1 \ge b + 1$. The result then follows from Theorem 2.6. □

Remark 3.7 *Let $f(x) \in \mathbb{F}_q[x]$. Since $\mathrm{ord}(f(x)) \ge \deg(f(x))$, by applying Theorem 2.7 one can improve the upper bound for $a_l + a_r$, i.e. $a_l + a_r < m(t - u) \le \mathrm{ord}(M_{a+1}(x) \cdots M_b(x))$.*

We now construct QSCs from the sum of BCH codes.

Theorem 3.8 *Let $n \ge 3$ be an integer such that $\gcd(n, 2) = 1$ and suppose that $2^{\lfloor m/2 \rfloor} < n \le 2^m - 1$, where $m = \mathrm{ord}_n(2)$. Consider integers a, b, e and f such that $2 \le e < a < b < f <$*

$\min\{\lfloor n2^{\lceil m/2\rceil}/(2^m-1)-1\rfloor, n-1, \lfloor\kappa\rfloor\}$, *where* $\kappa = \frac{n}{2^m-1}(2^{\lceil m/2\rceil}-1)$ *and* $a, b, e, f \not\equiv 0 \bmod 2$. *Then, for any pair of nonnegative integers* (a_l, a_r) *satisfying* $a_l + a_r < m(t-w)$, *there exists an* $(a_l, a_r) - [[n + a_l + a_r, n - 2m(t+1)]]$ *QSC that corrects up to at least* $\lfloor\frac{d-1}{2}\rfloor$ *phase errors and up to at least* $\lfloor\frac{d^*-1}{2}\rfloor$ *bit errors, where* $d \geq b+1$, $d^* \geq e+1$, $t = (b-1)/2$ *and* $w = (e-1)/2$.

Proof. Let C_1 be the binary narrow-sense BCH code of length n generated by the product of the minimal polynomials

$$C_1 = \langle M^{(1)}(x)M^{(3)}(x)\cdots M^{(b)}(x)\rangle,$$

where $b = 2t+1$ and $t \geq 0$. Let C_2 be the binary narrow-sense BCH code of length n generated by the product of the minimal polynomials

$$C_2 = \langle M^{(1)}(x)M^{(3)}(x)\cdots M^{(a)}(x)\rangle,$$

where $a = 2u+1$ and $u \geq 1$. From the construction $C_1 \subset C_2$, and by Proposition 3.4 C_1 is dual-containing. Further, consider the binary narrow-sense BCH codes of length n generated by

$$C_3 = \langle M^{(1)}(x)M^{(3)}(x)\cdots M^{(f)}(x)\rangle,$$

and

$$C_4 = \langle M^{(1)}(x)M^{(3)}(x)\cdots M^{(e)}(x)\rangle,$$

where $f = 2v+1$ with $v \geq 1$, and $e = 2w+1$ with $w \geq 0$. From the construction we have $C_3 \subsetneq C_4$. It then follows that $C_1 + C_3 \subsetneq C_2 + C_4$. Since $e < a$ and $b < f$, from Lemma 3.5 and a straightforward computation, the codes $C_2 + C_4$ and $C_1 + C_3$ have dimensions $K_2 = n - m(w+1)$ and $K_1 = n - m(t+1)$, respectively. The dimension of the corresponding QSC is $K = n - 2m(t+1)$ and $K_2 - K_1 = m(t-w)$. Since C_1 is dual-containing, proceeding similar to the proof of Theorem 3.1, it follows that $C_1 + C_3$ is also dual-containing. From the BCH bound, the minimum distance d_{13} of $C_1 + C_3$ satisfies $d_{13} \geq b+1$ and the minimum distance d_{24} of $C_2 + C_4$ satisfies $d_{24} \geq e+1$. Applying Theorem 3.1 to the codes $C_1 + C_3$ and $C_2 + C_4$, the result follows. $\square$

3.3 Quantum Synchronizable Codes From Duadic Codes

The duadic codes are a subclass of cyclic codes, and are a generalization of quadratic residue codes. Smid [22] characterized duadic codes based on the existence of a splitting. Duadic codes are important because they are related to self-dual and isodual codes [10].

As mentioned in Section 1, Zhang and Ge [24] constructed algebraic synchronizable codes from duadic codes of length p^n. Here we provide a more general result by considering duadic codes of length n, where n is a product of prime powers. We first recall some results on duadic codes.

Let S_1 and S_2 be unions of 2-cosets modulo m such that $S_1 \cap S_2 = \emptyset$, $S_1 \cup S_2 = \mathbb{Z}_m \setminus \{0\}$ and $\mu_a S_i \bmod m = S_{(i+1) \bmod 2}$. The triple μ_a, S_1, S_2 is called a splitting modulo m. The odd-like duadic codes D_1 and D_2 are the cyclic codes over $\mathbb{F}_2$ with defining sets S_1 and S_2, respectively, and generator polynomials $f_1(x) = \Pi_{i \in S_1}(x - \alpha^i)$ and $f_2(x) = \Pi_{i \in S_2}(x - \alpha^i)$, respectively. The even-like duadic codes C_1 and C_2 are the cyclic codes over $\mathbb{F}_2$ with defining sets $\{0\} \cup S_1$ and $\{0\} \cup S_2$, respectively. The cardinality of S_i is equal to $\frac{m-1}{2}$. If the splitting is given by μ_{-1}, then the minimum distance of the odd-like duadic codes satisfies $d^2 - d + 1 \geq m$. This is known as the square root bound.

Let m be an odd integer and denote the multiplicative order of 2 modulo m by $\mathrm{ord}_m(2)$. This order is equal to the degree of the minimal polynomial $M_1(x)$, and is the smallest integer l such that $2^l \equiv 1 \bmod m$.

In the following we give necessary and sufficient conditions for the existence of duadic codes. The notation $x \,\square\, y$ means that x is a quadratic residue modulo y.

Theorem 3.9 *[22] Duadic codes of length m over $\mathbb{F}_2$ exist if and only if $2 = \square \bmod m$. In other words, if $m = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$ is the prime factorization of m where $s_i > 0$, then duadic codes of length m over $\mathbb{F}_2$ exist if and only if $2 = \square \bmod p_i$, $i = 1, 2, \ldots, k$.*

The following lemma shows that under certain conditions on $\mathrm{ord}_q(2)$, there is a specific factorization of $x^m - 1$.

Lemma 3.10 *[11, Lemma 3.6] Let q be a prime power and m be an odd integer such that $\gcd(m, q) = 1$, and suppose that $\mathrm{ord}_m(q)$ is odd. Then any non-trivial irreducible divisor $M_i(x)$ of $x^m - 1$ in $\mathbb{F}_q[x]$ satisfies $M_i(x) \neq \alpha M_i^*(x)$. $\forall \alpha \in \mathbb{F}_q^*$.*

It can immediately be deduced from Lemma 3.10 that if m is an odd integer such that $\mathrm{ord}_m(2)$ is odd, then the polynomial $x^m - 1$ can be decomposed as

$$x^m - 1 = (x - 1) M_{i_1}(x) M_{i_1}{}^*(x) \cdots M_{i_s}(x) M_{i_s}{}^*(x). \tag{1}$$

We now investigate when a splitting modulo m, m an odd integer, is given by the multiplier μ_{-1}.

Proposition 3.11 *Let $m = p_1^{\alpha_1} \ldots p_l^{\alpha_l}$ be an odd integer such that, for all $i = 1, \ldots, l$, $p_i \equiv -1 \bmod 8$. Then the following hold:*

(i) all the splittings modulo m are given by μ_{-1}, and

(ii) there exists a pair of odd-like duadic codes D_i, $i = 1, 2$, generated by $g_i(x)$ such that $g_1(x) = g_2^*(x)$.

Proof. For part (i), since $p_i \equiv -1 \bmod 8$ for all $i = 1, \ldots, l$, it follows from [22, Theorem 8] that all the splitting are given by μ_{-1}. Part (ii) follows from part (i) and the decomposition in (1). $\square$

Proposition 3.12 *Assume that $m = {p_1}^{\alpha_1} \ldots {p_l}^{\alpha_l}$ is an odd integer such that, for all $i = 1, \ldots, l$, $p_i \equiv -1 \bmod 8$. Further assume that $T \subset \{i_1, \ldots, i_s\}$, where the i_j are as given in (1). Consider the cyclic code C with generator polynomial $g(x) = \prod_{j \in T} M_j(x)$. Then C is a dual-containing code.*

Proof. Let $m = {p_1}^{\alpha_1} \ldots {p_l}^{\alpha_l}$ be an odd integer such that, for all $i = 1, \ldots, l$, $p_i \equiv -1 \bmod 8$. Then $\mathrm{ord}_m(2) = \mathrm{lcm}(\mathrm{ord}_{p_i}(2))$, which is odd, and from (1), we have the decomposition $x^m - 1 = (x-1)M_{i_1}(x){M_{i_1}}^*(x) \ldots M_{i_s}(x){M_{i_s}}^*(x)$. Assume now that $g(x) = \prod_{i_j \in T} M_{i_j}(x)$ with $T = \{i_1, \ldots, i_t\}$, where $t \leq s$. The dual code of C has generator polynomial $g^{\perp}(x) = \frac{x^m-1}{\prod_{i_1 \leq i_j \leq i_t} M_{i_j}(x)^*}$. Hence, from (1), we obtain that $g^{\perp}(x) = (x-1)\prod_{i_j \leq t} M_{i_1}(x) \cdots M_{i_t}(x){M_{i_{t+1}}}^*(x) \cdots {M_{i_s}}^*(x)$, so $g | g^{\perp}$. Therefore $C^{\perp} \subset C$ as required. $\square$

Theorem 3.13 *Let $m = {p_1}^{\alpha_1} \ldots {p_1}^{\alpha_l}$ be an odd integer such that $p_i \equiv -1 \bmod 8$ for all $i = 1, \ldots, l$. Assume that $x^m - 1$ can be decomposed as $x^m - 1 = (x-1)M_{i_1}(x)M_{i_1}^*(x) \cdots M_{i_s}(x)$ ${M_{i_s}}^*(x)$, where the $M_{i_j}(x)$ are the minimal polynomials that are not self-reciprocal. Further, assume that $T' \subset T \subset \{i_1, \ldots, i_s\}$ are such that $\gcd(n; i_1; \ldots; i_t) = 1$ for all $i_j \in T$. Then for any pair of non-negative integers (a_l, a_r) satisfying $a_l + a_r < n$, with $n = \mathrm{ord}(h(x))$, where $h(x) = \prod_{i_j \in T \setminus T'} M_{i_j}(x)$ and n divides m, there exists an $(a_l, a_r) - [[m + a_l + a_r, m - 2\sum_{i_j \in T'} \deg(M_{i_j}(x))]]_2$ QSC that corrects up to at least $\lfloor \frac{d_1-1}{2} \rfloor \geq 1$ phase errors and up to at least $\lfloor \frac{d_2-1}{2} \rfloor \geq 1$ bit errors. Here, $d_2 \leq d_1$, where d_1 is the minimum distance of $C = \langle \prod_{i_j \in T} M_{i_j}(x) \rangle$ and d_2 is the minimum distance of $D = \langle \prod_{i_j \in T'} M_{i_j}(x) \rangle$.*

Proof. Under the assumption $\mathrm{ord}_m(2)$, we obtain the factorization of $x^m - 1$ from (1). Assume that $T \subset \{i_1, \ldots, i_s\}$, and let $g(x) = \prod_{i_j \in T} M_{i_j}(x)$. Now consider the cyclic code C generated by $g(x)$. From Proposition 3.12 we have that $C^{\perp} \subset C$.

Let D be the cyclic code generated by $h(x) = \prod_{i_j \in T'} M_{i_j}(x)$ with $T' \subset T$. Then we have that $C \subset D$. The polynomial $f(x) = \prod_{i_j \in T \setminus T'} M_{i_j}(x)$ has order n a divisor of m. From Lemma 2.5, the dimension of C is $k_1 = m - \sum_{i_j \in T} \deg(M_{i_j}(x))$, and the dimension of D is $k_2 = m - \sum_{i_j \in T'} \deg(M_{i_j}(x))$. Hence from Theorem 2.6, for any pair of non-negative integers (a_l, a_r) satisfying $a_l + a_r < n$, there exists an $(a_l, a_r) - [[m + a_l + a_r, m - 2\sum_{i_j \in T'} \deg(M_{i_j}(x))]]_2$

QSC that corrects up to at least $\frac{d_1-1}{2}$ phase errors and up to at least $\frac{d_2-1}{2}$ bit errors. The condition $\gcd(n; i_1; \dots; i_t) = 1$ for all $i_j \in T$ ensures that the minimum distances d_1 and d_2 of the codes C and D, respectively, are at least three [5]. $\square$

Corollary 3.14 *Let $m = {p_1}^{\alpha_1} \dots {p_1}^{\alpha_l}$ be an odd integer such that $p_i \equiv -1 \bmod 8$ for all $i = 1, \dots, l$. Then there exists a QSC with parameters $(a_r, a_l) - [[m + a_r + a_l, 1]]_2$ that can correct up to $\lfloor \frac{d_1-1}{2} \rfloor$ phase errors, where $d_1^2 - d_1 + 1 \geq m$, and can correct $\lfloor \frac{d_2-1}{2} \rfloor$ bits errors, with $d_2 \geq \frac{m-1}{2}$.*

Proof. Note that in this case we have $C = D_1 = \langle \prod_{1 \leq i_j \leq \frac{m-1}{2}} M_{i_j}(x) \rangle$ and $D = \langle \prod_{1 < i_j \leq \frac{m-1}{2}} M_{i_j}(x) \rangle$. If $f_1(x)$ and $g(x)$ are the generator polynomials of cyclic codes C and D, respectively, then $h(x) = f_1(x)/g(x) = M_1(x)$. Hence from [17, Theorem 3.5], the order of $h(x)$ equals $\mathrm{ord}_m(q)$. The minimum distance of $C = D_2$ is equal to d_1, since the splitting is given by μ_{-1}. The computation of d_1 follows from the square root bound whereas the minimum distance d_2 of D is obtained from the BCH bound. $\square$

Remark 3.15 *The codes given in Corollary 3.14 can only encode one qubit. Thus, even if the number of phase and bit errors which can be corrected is large, the code has very limited usefulness. To avoid this situation and to take advantage of the previous construction, repeated root cyclic codes (RRCCs) are considered in the next section to construct QSCs.*

3.4 Quantum Synchronizable Codes from Repeated Root Cyclic Codes

In [9], Fujiwara and Vandendriessche suggested that their results may be generalized to lengths other than $2^m - 1$. However, it is difficult to determine the order of the generator polynomial in the repeated root case. In this section, we show that the generalization of the construction of QSCs to the repeated root cyclic code (RRCC) case can be done easily. Further, employing RRCCs provides more flexibility and possibilities as a QSC can always be obtained. This generalization is possible due to the following remark.

Remark 3.16

- *The properties of cyclic codes used for encoding and decoding in the synchronization scheme suggested by Fujiwara et. al [8] are that a cyclic shift of a codeword is also a codeword and the polynomial representation of codewords. Hence when considering the codes C and D such that $(C)^{\perp} \subset C \subset D$ as RRCCs, the encoding and decoding does not have to change.*

- *The maximal tolerable magnitude of synchronization errors is related to the order of the polynomial $f(x)$ as follows. If $n = 2^{n'}m$, m odd, then we have $x^n - 1 = (x^m - 1)^{2^{n'}}$. Hence we obtain the factorization $x^n - 1 = f_1^{2^{n'}} \ldots f_l^{2^{n'}}$. If $f(x)$ is a power of an irreducible polynomial in $\mathbb{F}_2[x]$ which is a divisor of $x^m - 1$, then $f^{2^b}(x)|(x^{2^b m} - 1)$. From the definition one has*

$$\mathrm{ord}(f^{2^b}) = (\mathrm{ord}(f))^{2^b}. \tag{2}$$

  Hence, the order of any divisor $f(x)$ of $x^n - 1$ can be computed as the least common multiple of the order of the power of irreducible factors of $x^n - 1$ as done previously.

- *From the previous remark, the order of the polynomial $h(x)$ used in the construction of a code of length $2^a m$ is at most equal to $2^a \mathrm{ord}(h'(x))$ where $h'(x)$ is the product of all irreducible polynomials which divide $h(x)$. This makes the length of a QSC obtained from RRCCs larger by at most a factor 2^a. The next Theorem given by Castagnoli et al. [2] shows that while the length of the RRCC increases, the minimum distance may also increase by a factor P_t. Hence when using RRCCs to construct a QSC, we gain in the flexibility of choosing good codes in Theorems 2.6 and 2.7, and also gain in error correcting capability without a loss in the error rate d/n.*

Theorem 3.17 *[2, Theorem 1] Let C be a q-ary repeated root cyclic code of length $n = p^\delta m$, generated by $g(x)$, where p is the characteristic of $\mathbb{F}_q$, $\delta \geq 1$ and $\gcd(p, m) = 1$. Then $d_{min}(C) = P_t d_{min}(\overline{C_t})$ for some $t \in T$, where $\overline{C_t}$ is the cyclic code over $\mathbb{F}_q$ generated by $\overline{g_t}$ (the product of the irreducible factors of $g(x)$ that occur with multiplicity $e_i > t$, and $P_t = p^{j-1}(r+1)$, where r is such that $t = (p-1)p^{\delta-1} + \ldots + (p-1)p^{\delta-(j-1)} + rp^{\delta-j}$.*

Next, we extend the construction presented in Section 2 to RRCCs. We also show the importance of the flexibility in choosing codes with good minimum distance. While it is difficult and challenging to find dual-containing simple root cyclic codes, it is always possible to construct dual-containing repeated root cyclic codes. For instance, QSCs can always be constructed from cyclic codes of length $2n$, n odd, with $x^n - 1 = f(x)g(x)$. The dual of $f(x)$ is $f^\perp(x) = \frac{f(x)^{2*}g(x)^{2*}}{f^*(x)}$ and independent of $f^*(x)$, we always have that $f(x)|f^\perp(x)$. Hence the binary cyclic code of length $2n$ generated by $f(x)$ is dual-containing. From Theorem 3.17, the minimum distance of this code is the same as the minimum distance of the code of length n. If this minimum distance is good then there will not be a significant loss in the error rate.

Another interesting example is when the code length is $4n$. In this case, if $x^n - 1 = f(x)g(x)$ it can easily be shown that the code C of length $4n$ generated by $f^2(x)$ is dual-containing. Further, we have the inclusion $C \subset D$, where D is the cyclic code of length $4n$ generated by $f(x)$. Hence if $M_1(x)|f(x)$, then we have that $\mathrm{ord}(f) = 4n$. Applying Theorems 3.17 and 2.6 gives the following result.

Theorem 3.18 *Let n be an odd integer and assume that $x^n - 1 = f(x)g(x)$. Then for any pair of nonnegative integers (a_l, a_r) such that $a_l + a_r < 4n$, there exists an $(a_l, a_r) - [[4n, 4n - 2\deg(f(x))]]_2$ QSC that corrects at least $\frac{2d-1}{2}$ phase errors and at least $\frac{d-1}{2}$ bit errors, where d is the minimum distance of the cyclic code generated by $f(x)$.*

Table 1: Some examples of QSC obtained from Theorem 3.18

Linear Codes	Degree of f	QSC	Phase error	Bit error
$C = [n, k, d]_2$	$d^\circ f$	$Q_s = (a_l, a_r) - [[4 * n, 4 * n - 2d^\circ f]]_2$	$\lfloor \frac{2d-1}{2} \rfloor$	$\lfloor \frac{d-1}{2} \rfloor$
$[7, 4, 3]_2$	3	$(20, 5) - [[28, 22]]_2$	2	1
$[5, 1, 5]_2$	4	$(2, 5) - [[20, 12]]_2$	4	2
$[17, 9, 5]_2$	8	$(30, 8) - [[68, 52]]_2$	4	2
$[19, 1, 19]_2$	18	$(31, 13) - [[76, 40]]_2$	18	9
$[27, 9, 3]_2$	18	$(70, 15) - [[108, 72]]_2$	2	1
$[47, 24, 11]_2$	23	$(57, 113) - [[188, 142]]_2$	10	5
$[71, 36, 11]_2$	35	$(150, 23) - [[284, 214]]_2$	10	5
$[97, 49, 15]_2$	48	$(103, 215) - [[388, 292]]_2$	14	7
$[103, 52, 19]_2$	51	$(250, 91) - [[412, 310]]_2$	18	9

Remark 3.19 *If the splitting is given by μ_{-1}, then the corresponding duadic codes have good minimum distance. The following theorem is an extension of the construction given in Section 2.*

Theorem 3.20 *Let $m = {p_1}^{\alpha_1} \dots {p_1}^{\alpha_l}$ be an odd integer such that, for all $i = 1, \dots, l$, $p_i \equiv -1 \bmod 8$. Then for any pair of nonnegative integers (a_l, a_r) such that $a_l + a_r < 2m$, there exists an $(a_l, a_r) - [[2m, m-1]]_2$ QSC that corrects at least $\frac{d-1}{2}$ bit and phase errors, where $d^2 - d + 1 \geq m$.*

Proof. Let $m = {p_1}^{\alpha_1} \dots {p_1}^{\alpha_l}$ be an odd integer such that $p_i \equiv -1 \bmod 8$ for all $i = 1, \dots, l$. Then there exists a pair of odd-like duadic codes D_i, $i = 1, 2$, whose splitting is given by μ_{-1}. If $f_i(x)$ is the generator polynomial of D_i, then $x^m - 1 = (x-1)f_1(x)f_2(x)$, where ${f_1}^*(x) = f_2(x)$. Let C be the cyclic code of length $2m$ generated by $f(x) = (x-1)f_1(x)$. The dimension of C is $\frac{3m-1}{2}$. Further, the polynomial $f^{\perp}(x) = \frac{(x-1)^2 {f_1}^2 {f_2}^2}{(x-1){f_1}^*} = {f_1}^2 f_2$ generates the dual code $C^{\perp}$. If D is the cyclic code of length $2m$ generated by $f_1(x)$, it follows that $C^{\perp} \subset C \subset D$. From (2) and Lemma 2.5, one has that $\operatorname{ord} f(x) = 2m$. Since the splitting is given by μ_{-1}, the minimum distance of the duadic code is d, and this is also the minimum distance of the cyclic even-like duadic code of length m generated by $(x-1)f_1(x)$. From

the square root bound it follows that $d^2 - d + 1 \geq m$. Further, Theorem 3.17 gives that d is also the minimum distance of the codes C and D. $\square$

The construction and proof of Theorem 3.20 are valid when considering codes of length $2^i m$, which gives the following theorem.

Theorem 3.21 *Let $m = {p_1}^{\alpha_1} \ldots {p_l}^{\alpha_l}$ be an odd integer such that, for all $i = 1, \ldots, l$, $p_i \equiv -1 \bmod 8$. Then, for any pair (a_l, a_r) of nonnegative integers such that $a_l + a_r < 2^i m$, there exists an $(a_l, a_r) - [[2^i m, 2^i m - m - 1]]_2$ QSC that corrects at least $\frac{d-1}{2}$ bit and phase errors, where $d^2 - d + 1 \geq m$.*

4 Quantum Synchronizable Codes from Product Codes

The product code construction is a useful means of combining codes of different length. then in some cases the severe requirement on the cyclic codes (for example duadic and BCH codes) can be relaxed. We recall the direct product of linear codes. For more details we refer the reader to [19].

Let C_1 and C_2 be two linear codes with parameters $[n_1, k_1, d_1]_q$ and $[n_2, k_2, d_2]_q$, respectively, both over $\mathbb{F}_q$. Assume that $G^{(1)}$ and $G^{(2)}$ are the generator matrices of C_1 and C_2, respectively. Then the product code $C_1 \otimes C_2$ is a linear $[n_1 n_2, k_1 k_2, d_1 d_2]$ code over $\mathbb{F}_q$ generated by the Kronecker product matrix $G^{(1)} \otimes G^{(2)}$ defined as

$$G^{(1)} \otimes G^{(2)} = \begin{bmatrix} g_{11}^{(1)} G^{(2)} & g_{12}^{(1)} G^{(2)} & \cdots & g_{1n_1}^{(1)} G^{(2)} \\ g_{21}^{(1)} G^{(2)} & g_{22}^{(1)} G^{(2)} & \cdots & g_{2n_1}^{(1)} G^{(2)} \\ \vdots & \vdots & \vdots & \vdots \\ g_{k_1 1}^{(1)} G^{(2)} & g_{k_1 2}^{(1)} G^{(2)} & \cdots & g_{k_1 n_1}^{(1)} G^{(2)} \end{bmatrix}$$

Theorem 4.1 *Let n and n^* be two positive odd integers such that $\gcd(n, n^*) = 1$. Let C_1 be an $[n, k_1, d_1]$ self-orthogonal cyclic code and C_2 an $[n, k_2, d_2]$ cyclic code, both over $\mathbb{F}_2$. Consider that C_3 and C_4 are two cyclic codes with parameters $[n^*, k_3, d_3]$ and $[n^*, k_4, d_4]$, respectively, over $\mathbb{F}_2$ such that $(C_1 \otimes C_3)^\perp \subsetneq C_2 \otimes C_4$. Then for any pair of nonnegative integers (a_l, a_r) satisfying $a_l + a_r < k_1 k_3 + k_2 k_4 - n n^*$, there exists an $(a_l, a_r) - [[n n^* + a_l + a_r, n n^* - 2k_1 k_3]]$ QSC that corrects up to at least $\lfloor \frac{d-1}{2} \rfloor$ phase errors and up to at least $\lfloor \frac{d_2 d_4 - 1}{2} \rfloor$ bit errors, where d is the minimum distance of the code $(C_1 \otimes C_3)^\perp$, which satisfies $d \geq d_2 d_4$.*

Proof. Since $\gcd(n, n^*) = 1$, it follows that the product code $C_2 \otimes C_4$ (consequently, $C_1 \otimes C_3$ and $(C_1 \otimes C_3)^\perp$) is also cyclic [19, Theorem 1, Page 570]. The elements of the code $C_1 \otimes C_3$ are linear combinations of vectors $v_i^{(1)} \otimes w_j^{(3)}$, where $v_i^{(1)} \in C_1$ and $w_j^{(3)} \in C_3$, i.e.

every $c \in C_1 \otimes C_3$ can be written as $c = \sum_i v_i^{(1)} \otimes w_i^{(3)}$. An (Euclidean) inner product on $C_1 \otimes C_3$ is defined as

$$\langle v_i^{(1)} \otimes w_i^{(3)} | v_j^{(1)} \otimes w_j^{(3)} \rangle = \langle v_i^{(1)} | v_j^{(1)} \rangle \langle w_i^{(3)} | w_j^{(3)} \rangle, \tag{3}$$

and it is extended by linearity for all elements of $C_1 \otimes C_3$. Note that $\langle c_i^{(1)} | c_j^{(1)} \rangle$ and $\langle c_i^{(3)} | c_j^{(3)} \rangle$ are the Euclidean inner products on C_1 and C_3, respectively. From (3), since C_1 is self-orthogonal, $C_1 \otimes C_3$ is also self-orthogonal, so $(C_1 \otimes C_3)^{\perp}$ is dual-containing. The parameters of the codes $(C_1 \otimes C_3)^{\perp}$ and $C_2 \otimes C_4$ are $[nn^*, nn^* - k_1k_3, d]$ and $[nn^*, k_2k_4, d_2d_4]$, respectively. Since $(C_1 \otimes C_3)^{\perp} \subsetneq C_2 \otimes C_4$, it follows that $d \geq d_2d_4$. Applying Theorem 2.6 to the cyclic codes $(C_1 \otimes C_3)^{\perp}$ and $C_2 \otimes C_4$, the result follows. □

Acknowledgements

The authors would like to thank H. Zitouni for constructing the codes in Table 1. G.G. La Guardia has been partially supported by the Brazilian Agencies CAPES and CNPq.

References

[1] S.A. Aly and A. Klappenecker. On quantum and classical BCH codes. *IEEE Trans. Inform. Theory*, 53(3):1183–1188, 2007.

[2] G. Castagnoli, J.L Massey, P. Schoeller and N. Von Seemann. On repeated-root cyclic codes. *IEEE Trans. Inform. Theory*, 37(2):337–342, 1991.

[3] R.C. Bose and D.K. Ray-Chaudhuri. Further results on error correcting binary group codes. *Information and Control*, 3:279–290, 1960.

[4] R.C. Bose and D.K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Inform. Control*, 3:68–79, 1960.

[5] P. Charpin, A. Tietäväinen and V. Zinoviev. On binary cyclic codes with minimum distance $d = 3$. *Prob. Inform. Transmission*, 33(4):287–296, 1997.

[6] M.F. Ezerman, S. Ling and P. Solé. Additive asymmetric quantum codes. *IEEE Trans. Inform. Theory*, 57(8):5536–5550, 2011.

[7] Y. Fujiwara. Block synchronization for quantum information. *Phys. Rev. A*, 87(02):23–44, 2013.

[8] Y. Fujiwara, V.D. Tonchev and T.W.H. Wong. Algebraic techniques in designing quantum synchronizable codes. *Phys. Rev. A*, 88(1):012318, 2013.

[9] Y. Fujiwara and P. Vandendriessche. Quantum synchronizable codes from finite geometries. *IEEE Tran. Inform. Theory*, 60(11):7345–7354, 2014.

[10] K. Guenda. Quantum duadic and affine-invariant codes. *Int. J. Quantum Inform.*, 7(1):373–384, 2009.

[11] K. Guenda and T.A. Gulliver. Self-dual repeated root cyclic and negacyclic codes over finite fields. In *Proc. IEEE Int. Symp. Inform. Theory*, 2914–2918, 2012.

[12] K. Guenda and T.A. Gulliver. Symmetric and asymmetric quantum codes. *Int. J. Quantum Inform.*, 11(5):1350047, 2013.

[13] W.C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes.* Cambridge Univ. Press, New York, 2003.

[14] L. Ioffe and M. Mézard. Asymmetric quantum error-correcting codes. *Phys. Rev. A*, 75(3):032345, 2007.

[15] G.G. La Guardia. Asymmetric quantum Reed-Solomon and generalized Reed-Solomon codes. *Quantum Inform. Process.*, 11:591–604, 2012.

[16] G.G. La Guardia. Asymmetric quantum codes: New codes from old. *Quantum Inform. Process.*, 12:2771–2790, 2013.

[17] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and their Applications.* Cambridge Univ. Press, Cambridge, UK, 1975.

[18] R. Lidl and H. Niederreiter. *Finite Fields.* Cambridge Univ. Press, Cambridge, UK, 1997.

[19] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, 1977.

[20] M. Probst and L. Trieloff. Bit and Frame Synchronization Techniques, 2003.

[21] P.K. Sarvepalli, A. Klappenecker and M. Rotteler. Asymmetric quantum codes: Constructions, bounds and performance. *Proc. R. Soc. A*, 465(2105):1645–1672, 2009.

[22] M.H.M. Smid. Duadic codes. *IEEE. Trans. Inform. Theory*, 33(3):432–433, May 1987.

[23] X. Yixuan, J. Yuan and Y. Fujiwara. Quantum synchronizable codes from quadratic residue codes and their supercodes. In *Proc. IEEE Inform. Theory Workshop*, Hobart, TAS, 172–176, Nov. 2014.

[24] T. Zhang and G. Ge. Quantum block and synchronizable codes derived from certain classes of polynomials. Available online: http://arxiv.org/abs/1508.00974.